



DEPARTMENT OF THE NAVY
NAVY PERSONNEL COMMAND
5720 INTEGRITY DRIVE
MILLINGTON TN 38055-0000

NAVPERSCOMINST 2200.1B

PERS-334

16 DEC 2008

NAVPERSCOM INSTRUCTION 2200.1B

From: Commander, Navy Personnel Command

Subj: HANDLING AND CONTROL OF ELECTRONIC KEY MANAGEMENT
SYSTEM 1A (EKMS 1A)

Ref: (a) Electronic Key Management System 1 (EKMS 1A)
(b) NAVPERSCOMINST 2200.2A
(c) NAVPERSCOMINST 2200.3B
(d) SECNAV M-5510.30 of 1 Jun 06
(e) SECNAV M-5510.36 of 1 Jun 06
(f) U.S. Navy Regulations, 1990

Encl: (1) Sample COMSEC User Responsibility Acknowledgement
Form
(2) Sample Local Element Access Letter

1. Purpose. To establish program regulations and procedures per references (a) through (f) for the handling, distribution, and control of Communications Security (COMSEC) material within Navy Personnel Command (NAVPERSCOM) using the Electronic Key Management System (EKMS). This instruction has been substantially changed and should be read in its entirety.

2. Cancellation. NAVPERSCOMINST 2200.1A.

3. Information. Reference (a) prescribes the policies and procedures for issuing, accounting, handling, safeguarding, and disposing of COMSEC material and the application of cryptographic and physical security measures to COMSEC material and facilities. Reference (b) provides information, establishes policies, handling, and procedures for secure telephone equipment (STE). Reference (c) establishes policies and procedures for the Emergency Action Plan (EAP) for the command. Reference (d) provides all Department of the Navy (DON) commands, activities, and personnel with regulations and guidance governing the DON Personnel Security Program (PSP). Reference (e) establishes uniform DON Information Security

Program (ISP) policies and procedures. EKMS 1 provides the capability for automated generation, accounting, distribution, destruction, and management of electronic key, as well as management of physical key and non-key COMSEC related items.

4. Scope. This instruction is promulgated per reference (a) but in no way alters or amends the provisions of references (b) through (f).

5. Responsibilities

a. Staff COMSEC Responsibility Officer (SCMSRO). The SCMSRO is responsible for:

(1) The proper management and security of all COMSEC material.

(2) Ensuring compliance with established policy and procedures governing the safeguarding and handling of COMSEC material.

(3) Appointing, in writing, qualified and responsible individuals as the EKMS manager and alternate manager(s) and, if desired, an EKMS clerk.

(4) Establishing, in writing, a list of personnel authorized access to keying material.

(5) Ensuring that unannounced quarterly spot checks of the EKMS vault and spaces are conducted to ensure COMSEC material is properly used and stored. Reference (a) contains a complete list of the SCMSRO's responsibilities for COMSEC material held by the account.

b. EKMS Manager. EKMS manager is responsible to the SCMSRO for the proper management and security of all COMSEC material held at the command, and serves as the SCMSRO's primary advisor on EKMS account management.

c. Alternate EKMS Manager. Alternate EKMS manager(s) are jointly responsible with the EKMS manager to the SCMSRO for the proper management and security of all COMSEC material held by the command and, as such, has the same duties and responsibilities as the EKMS manager. On a continuing basis,

16 DEC 2008

the alternate managers must be actively involved in the daily operation of the account and is ready at all times to administer the account in the absence of the EKMS manager.

d. Command Relationships

(1) Management and security of COMSEC material are inherent responsibilities at all levels of the command. Proper evaluation of EKMS administrative procedures can be made only if officials in the operational chain of command understand EKMS procedures and requirements; therefore, officials in the chain of command who are senior to the EKMS manager, or to the local elements, must be familiar with EKMS account operations and must be involved in the management of COMSEC material and security requirements.

(2) In performing routine duties, the EKMS manager will normally report to NAVPERSCOM (PERS-334) for functional direction and administration; however, they have direct access to the SCMSRO.

e. Local Elements (LEs). The LEs are responsible for the proper security, control, accountability, and disposition of the COMSEC material placed in their charge and must comply with the procedures in references (a) and (b) and this instruction. All LEs must execute the EAP, reference (c), annually and each user must complete the COMSEC User Responsibility Acknowledgment letter, enclosure (1). LEs will submit an LE access letter on all personnel who have access to COMSEC material and/or equipment including STE telephones, enclosure (2). All LE users will attend monthly stand up training and respond to monthly e-mail training provided by the EKMS Manager.

f. COMSEC Witness. Any government employee (military or civilian) may be a COMSEC witness, provided the individual has an appropriate security clearance, a need-to-know, proper security access, and training from the EKMS manager. They may witness destruction, enter amendments, conduct page checks, or witness the inventory of COMSEC material. An individual who witnesses a COMSEC inventory, destruction of other COMSEC reports, or local COMSEC records is equally responsible for the accuracy of information, the physical citing of material to be destroyed or inventoried, and the timeliness familiarization

with the applicable procedures in reference (a) and this instruction.

6. Access. Only those persons properly cleared who have a need-to-know are granted access to COMSEC material. In addition, two-person integrity (TPI) will apply to COMSEC material from initial time of receipt at the EKMS account through issuance to local elements, or destruction. TPI means no single person will at any time, regardless of grade or status, be allowed access to Top Secret COMSEC keying material without the presence of another person formally authorized access to COMSEC material.

7. Issue of Material. Use SF-153, COMSEC Material Report, and the EKMS-generated COMSEC material report to document transactions on receipt or return of COMSEC material between the EKMS manager and LEs. Two COMSEC users must sign the SF-153.

8. Storage of COMSEC Material

a. Storage spaces for COMSEC material will provide maximum protection against unauthorized access, material damage, or deterioration. They must be secured when not under direct supervision of properly cleared and authorized personnel. Storage containers for COMSEC material outside the COMSEC vault will be approved by the EKMS manager and must meet the requirement of reference (a).

b. In stowing COMSEC material, consider arranging the material for ease of handling and emergency destruction. Separate Top Secret COMSEC material from other classifications, regardless of status marking. The minimum separation in status order is:

- (1) Effective keying material.
- (2) Reserve on-board (ROB) keying material.
- (3) When directed (WHENDI) material.
- (4) Combinations to EKMS account storage and containers.

c. Per reference (d), change combinations of containers used to store COMSEC material.

(1) When a person having knowledge of the combination no longer requires access.

(2) When the combination becomes, or is suspected to have been, compromised.

(3) Twenty-four months from the date of the last change.

(4) When the container is placed in use.

(5) When the container is taken out of service.

d. Access to Combinations

(1) Knowledge of the combinations to the EKMS account safes is limited to the EKMS manager and alternate EKMS manager(s).

(2) To provide for emergency access, a central record of the lock combinations for all COMSEC material security containers must be maintained in a security container (other than the container where COMSEC material is stored) approved for storage of the highest classification of the material protected by the combinations locks.

(3) Knowledge of combinations to safes containing COMSEC material held by LEs is limited to cleared personnel with a need-to-know.

(4) Combinations to containers used to store COMSEC material are held and made known only to the designated EKMS manager and alternate(s). Reference (a), article 515, contains detailed instructions for access to these combinations. Ensure each combination is recorded separately and protectively packaged in separate envelopes; store both envelopes in the same container; wrap each combination separately in aluminum foil; and laminate the envelope in plastic or seal with plastic tape.

e. Reproduction. Per reference (a), the EKMS manager is the only person authorized to reproduce COMSEC material.

f. Damaged, Worn, or Mutilated Publications. Return such publications to the EKMS manager for replacement.

g. Amendments, Changes, and Corrections

(1) When an amendment or correction to COMSEC material is provided to an LE, the EKMS manager will also include a copy of reference (a), figures 7-4 and 7-5 of article 787, as a check-off guide. The LE will enter the amendment per article 787 immediately after receipt.

(2) Page-check the basic publication following entry of an amendment that removes, substitutes, or adds pages. The individual who entered the amendment makes a page-check and the individual who verified the entry makes a second, complete page-check. Both of these page-checks are recorded on the publication's "Record of Page-checks" as separate entries.

(3) Be extremely careful to ensure amendments and corrections are not entered before their effective dates.

(4) Handle amendment residue by local destruction record and certification of proper entry with written notification to the EKMS manager per reference (a), figure 7-5.

h. Accountability Legend Codes (ALC)

(1) ALC is a numeric code used to determine how COMSEC material is accounted for within the COMSEC. ALC is used to identify the minimum accounting controls required for COMSEC material. The degree of accountability required for each ALC is explained as follows:

(a) ALC-1. COMSEC material is continuously accountable and must be accounted for by serial/register number from production to destruction.

(b) ALC-2. COMSEC material is continuously accountable by quantity from production to destruction.

(c) ALC-4. COMSEC material is locally accountable by quantity and handled or safeguarded based on its classification after initial receipt to Director, Communication Material System (DCMS).

(d) ALC-6. COMSEC material is electronically generated and is continuously accountable to the central office

of record (COR) by short title and accounting number from
~~production to destruction.~~

(e) ALC-7. COMSEC material is electronically generated and is accountable to the generation facility. All key transfers, including all subsequent transfers, must also be reported to the generating facility.

i. Procedures for Destroying COMSEC Material in Paper Form

(1) Destruction Procedures. The EKMS manager, alternate manager, or LE and a properly cleared COMSEC witness will destroy keying material per the following procedures:

(a) The COMSEC material for destruction will be separated from all other similar COMSEC material. All COMSEC material to be retained will be removed from the general area in which destruction will take place.

(b) Two individuals will verify the short titles and accounting data of the COMSEC material for destruction in the following manner:

1. The person responsible for conducting the destruction will read the short titles, editions suffix (if any), accounting numbers, and segment numbers to the witness who will mark the appropriate entries on the destruction record. To preclude inadvertent or unauthorized destruction of COMSEC material, and ensure pages or segments are not stuck together.

2. In turn, the COMSEC witness will read the short titles, edition suffix (if any), accounting numbers, and segment numbers to the person responsible for conducting the destruction and making appropriate entries on the destruction record.

(c) Immediately after verifying the accuracy and completeness of the line entries, one person will insert the material into the shredder (or other approved destruction method) while the other person watches.

(d) Keymat stored in a Data Transfer Device (DTD), will be zeroized per EKMS standard operating procedures issued. Immediately after verifying the accuracy and completeness of the

zeroization, sign a CMS 25 form for segmented material and an SF-153 for annual material.

(2) Loss of Keying Material

(a) Stop all destruction procedures immediately.

(b) Search the entire area.

(c) Re-check all keying material that has been used and the remaining key material.

(d) Contact the EKMS manager or the primary alternate EKMS manager IMMEDIATELY if material cannot be located.

j. Emergency Action Plan (EAP). Per reference (c), the EKMS account manager will ensure a detailed EAP for all COMSEC material is prepared and updated periodically. Since a natural disaster or emergency will not normally represent an attempt by hostile forces to capture cryptographic material, planning and actions will be directed to maintaining control over the material until the incident has passed or to moving the most sensitive material to a safer area. In case of fire, primary consideration is the safety and welfare of personnel. If safely securing or removing classified material is not possible, leave material in place to be consumed by fire. Under no circumstances will personnel subject themselves or their subordinates to injury or death to protect these materials from fire. If emergency destruction is ordered, the LE will destroy COMSEC material by methods approved for routine destruction of COMSEC material. The LE will then report the destruction to the EKMS manager. All commands that have entered into an MOA with NAVPERSCOM must have a separate EAP.

k. COMSEC Incident. Actual or suspected loss or compromise of COMSEC material shall be reported IMMEDIATELY to the EKMS manager who will notify the SCMSRO and take required action and make required reports.

l. Removal and movement of COMSEC Material. Under no circumstances will COMSEC material be removed from the command by anyone other than the EKMS Manager and alternates. COMSEC

material/equipment will not be moved unless EKMS manager has authorized the move.

m. Extracts of COMSEC Material

(1) To satisfy an emergent operational requirement, the SCMSRO may authorize the preparation of extracts from any COMSEC material held by the account.

(2) During non-emergency situations, sources that constitute authorization for preparing classified extracts are:

(a) Letter of Promulgation (LOP), Handling Instruction (HI), forward page, or text of the publication.

(b) Separately issued directive affecting a series of publications.

(c) Controlling authority of the material when the named resources do not address extraction.

n. Sealing COMSEC Material. Unsealed COMSEC material, at the EKMS manager or LE level, after its initial page check, will be sealed or resealed by the user per reference (a), article 772.

o. Inventory Requirements

(1) Short title, edition, accounting number, and quantity will list the material.

(2) Inventory all paper keying material by citing its short title, edition, and accounting number. Equipment may be inventoried by quantity only.

(3) The inventory must be designated to provide a means of recording dates and initials or signatures to certify that the inventory was conducted.

(4) An inventory of all COMSEC material held is required during each watch turnover unless a waiver has been granted in writing by Naval Communications Security Material System. If a waiver has been received, a complete inventory will be conducted on a daily basis or watch to watch basis.

(5) Conduct the inventory with appropriately cleared and authorized personnel. (Note: In the case of COMSEC material requiring TPI, two individuals completing the inventory must sign the inventory.)

9. COMSEC Terms and Definitions. All terms and definitions are located in EKMS 1, annex A.

10. Action. The EKMS manager will ensure COMSEC administrative personnel and LEs understand their responsibilities and are sufficiently trained. The EKMS manager shall monitor the overall internal security, accountability, and destruction of COMSEC material, and shall provide guidance when required. To aid in the proper maintenance of the EKMS account, COMSEC advice and assistance visits are required every 18 months as requested by the command EKMS manager.

11. Storage Containers. Storage containers for COMSEC material require the following and are available from NAVPERSCOM (PERS-334H):

a. An SF 700, Classified Container Information, must be placed on the inside of each COMSEC storage container.

(1) Privacy act information, e.g., address, social security number (last four digits), excluded from the SF 700, must be replaced with a statement such as, "Contact duty office" or "See command recall bill" unless a release statement has been signed by the individual(s) involved.

(2) A copy of the release statement must be maintained on file.

b. An SF 702, Security Container Check Sheet must be maintained for each lock on the COMSEC storage container.

c. An OF 89, Maintenance Record for Security Containers/Vault Doors, must be maintained for each COMSEC storage container/vault door. This is a permanent record and must be placed with the container. When maintenance is preformed on safe/vault this form will be filled out.

d. An SF 153, COMSEC Material Report, and all COMSEC and container forms will be provided by NAVPERSCOM (PERS-334H).

16 DEC 2008

12. Forms

a. Following forms are available at:
<http://www.dtic.mil/whs/directives/infomgt/forms/sfofforms.htm>.

(1) SF 702 (08-85), Security Container Check Sheet.

(2) SF 153 (09-88), COMSEC Material Report.

b. Following forms are available from NAVPERSCOM (PERS-334H):

(1) SF 700 (45-01), Security Container Information Instructions.

(2) OF 89 (9-98), Maintenance Record for Security Containers/Vault Doors.



ANN STEWART

Deputy

Distribution:

Electronic only, via NAVPERSCOM Web site

<https://www.npc.navy.mil/audiences/forinternal>

SAMPLE COMSEC USER RESPONSIBILITY ACKNOWLEDGMENT LETTER

(Date)

From: _____
(Rank/Rate/Grade First, Middle Initial, Last Name, last
four of SSN)
To: Navy Personnel Command (PERS-334H)
Subj: COMMUNICATIONS SECURITY (COMSEC) USER RESPONSIBILITY
ACKNOWLEDGMENT
Ref: (a) EKMS-1A
(b) NAVPERSCOMINST 2200.1B
(c) SECNAV M-5510.30 of 1 Jun 06
(d) SECNAV M-5510.36 of 1 Jun 06
(e) U.S. Navy Regulations, 1990

1. I hereby acknowledge that I have read and understand references (a) through (e).
2. I assume full responsibility for the proper handling, storage, inventorying, accounting, transfer, destruction and disposition of COMSEC material held in my custody and used by me and personnel under my supervision. I have knowledge of and will keep myself informed of pertinent articles in reference (a) through (e) that set forth policies, procedures, and responsibilities for safeguarding COMSEC material.
3. I have received a copy of reference (a) from the EKMS manager. If at anytime I am in doubt as to the proper handling of COMSEC material, I will immediately contact the EKMS manager at 874-5353 and request advice. I will attend EKMS training when required.
4. Before I detach I will report to the EKMS manager and be relieved of responsibility for all COMSEC material in my custody. My projected rotation date is _____.
(DDMMYYYY)

Enclosure (1)

NAVPERSCOMINST 2200.1B
16 DEC 2008

Subj: COMMUNICATIONS SECURITY (COMSEC) USER RESPONSIBILITY
~~ACKNOWLEDGMENT~~

5. The following is requested:

E-mail address: _____

Building #: _____ Room #: _____ Phone #: _____

Command: _____

(Signature)

16 DEC 2008

SAMPLE LOCAL ELEMENT ACCESS LETTER

(DDMMYYY)

From: (Name of Local Element)
 To: Electronic Key Management System (EKMS) Manager
 Subj: LOCAL ELEMENT ACCESS TO COMMUNICATION SECURITY (COMSEC)
 AND SAFE
 Ref: (a) NAVPERSCOMINST 2200.1B

1. Per reference (a), the following personnel are authorized EKMS users and have access to crypto equipment/material and secure telephone equipment card stored in local element safe NAVPERSCOM 02:

<u>NAME</u>	<u>RANK</u>	<u>SSN</u>	<u>CLEARANCE</u>
Smith, Tammy E.	LCDR	XXX-XX-7890	Secret
Johnson, David L.	PSC	XXX-XX-5432	Secret

Tammy E. Smith
 NAVPERSCOM (PERS-40)
 Point of Contact